

Generalized Controlled Quantum Secure Communication using GHZ-like state

Jemy Geordy*, Dintomon Joy† and Sabir M‡

*Department of Physics, Cochin University of Science and Technology,
Kochi - 682 022, India*

July 27, 2016

Abstract

We present a novel scheme for controlled quantum secure communication (CQSC) using GHZ-like state. In this scheme, a trusted controller assists the users for achieving secure transmission of data between them. The dense coding technique is exploited to increase the qubit efficiency and we show that the proposed scheme is immune against common eavesdropping attacks. We show how the method can be generalized to include N controllers using sets of GHZ-like states shared among the controllers and users. In this process entanglement swapping and single particle measurements are performed by the controllers to relax their controls and the users get entangled in Bell states.

1 Introduction

Quantum Cryptography has emerged as area of research in recent times. It is recognized that quantum processors can supersede current cryptographic protocols and offer highly secure cryptographic protocols for quantum communication. In 1984, Bennett and Brassard[1] proposed the pioneering work in Quantum Key Distribution (QKD), popularly known as BB84 protocol. This work motivated the scientific community to exploit the intriguing features of quantum mechanics to get more secure and efficient cryptographic protocols. In QKD, initially a secret quantum key is established between communicating parties and then this key is used for encryption and decryption of the message which is sent classically by Alice(sender) to Bob(receiver). With further developments in quantum cryptography, two other kinds of protocols were proposed. These are the quantum secure direct communication(QSDC)[2, 3, 4] scheme and the deterministic secure quantum communication(DSQC)[5, 6, 7] scheme. Unlike QKD, the QSDC and DSQC techniques do not require previously shared key for communication: the secret messages are communicated directly. However,

*jemygeordy@gmail.com

†dintomonjoy@cusat.ac.in

‡msr@cusat.ac.in

there is a slight difference between QSDC and DSQC. The later requires at least one bit of classical information to decode each qubit of the secret message and in the case of QSDC there is no requirement of any additional classical bit to decode the secret message[8, 9, 10]. Different QSDC and DSQC schemes have been proposed employing different entangled states such as EPR pairs[7, 11], GHZ states[5, 12], GHZ-like states[8, 13], W states[14, 15] etc. Moreover, there are schemes employing different methods such as dense coding[4], entanglement swapping[5], teleportation[6] etc for transmitting the secret message.

Recently, another kind of quantum communication scheme with the inclusion of a controller who controls the whole communication has been put forward by many research groups[9, 10, 13, 16]. In this scheme, designated as Controlled Quantum Secure Direct Communication(CQSDC), the co-operation of the controller is essential for the successful communication between the legitimate users. In practical situations all users prefer a smaller system than the service provider. Therefore, it is meaningful to have a controller to prepare the state when it is needed for communication and have a control over the communication without the capability of accessing the secret message. In a recent work, Pathak[10] pointed out that, since in the proposed methods an additional classical bit from the controller is required to decode the secret message, it is more appropriate to name this as CDSQC (Controlled Secure Direct Quantum Communication) instead of CQSDC.

In this paper we propose a new controlled quantum communication protocol making use of GHZ-like states[17, 18] and dense coding[19]. This is achieved by exploiting a unique GHZ-like state: the entanglement between two particles remain even after a measurement is made on one of the particles[9, 20]. Since, in the proposed scheme the communication between the legitimate users start only after receiving a classical bit from the controller, we designate our protocol as Controlled Quantum Secure Communication(CQSC), eventhough the communication as such is purely QSDC. The generalization of our protocol to N number of controllers is presented, where the controllers perform entanglement swapping also.

This paper is organized as follows. In section 2, we describe the CQSC using a GHZ-like state and dense coding. In section 3 we extend our scheme to CQSC with two controllers and in section 4 with three controllers. In section 5 the method is generalized to the case of N number of controllers (MCQSC). Analysis of the security and efficiency of the proposed CQSC protocol is given in section 6. Our conclusions are presented in section 7.

2 Controlled Quantum Secure Communication using a GHZ-like state

A GHZ-like state can be prepared from a single qubit state, Bell pair with a controlled-NOT operation as given in references[8, 9]. The set of eight orthonor-

mal GHZ-like states[9] is given by,

$$\begin{aligned} |\zeta_{000}\rangle &= \frac{1}{\sqrt{2}}[|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle], & |\zeta_{001}\rangle &= \frac{1}{\sqrt{2}}[|\phi^+\rangle|1\rangle + |\psi^+\rangle|0\rangle] \\ |\zeta_{010}\rangle &= \frac{1}{\sqrt{2}}[|\phi^+\rangle|0\rangle - |\psi^+\rangle|1\rangle], & |\zeta_{011}\rangle &= \frac{1}{\sqrt{2}}[|\phi^+\rangle|1\rangle - |\psi^+\rangle|0\rangle] \\ |\zeta_{100}\rangle &= \frac{1}{\sqrt{2}}[|\phi^-\rangle|0\rangle + |\psi^-\rangle|1\rangle], & |\zeta_{101}\rangle &= \frac{1}{\sqrt{2}}[|\phi^-\rangle|1\rangle + |\psi^-\rangle|0\rangle] \\ |\zeta_{110}\rangle &= \frac{1}{\sqrt{2}}[|\phi^-\rangle|0\rangle - |\psi^-\rangle|1\rangle], & |\zeta_{111}\rangle &= \frac{1}{\sqrt{2}}[|\phi^-\rangle|1\rangle - |\psi^-\rangle|0\rangle] \end{aligned}$$

where, $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ represents the Bell states.

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle], \quad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$$

In this protocol, we consider Alice as the sender who wants to send secret message to Bob the receiver and Charlie controls the communication. The proposed CQSC consists of the following steps,

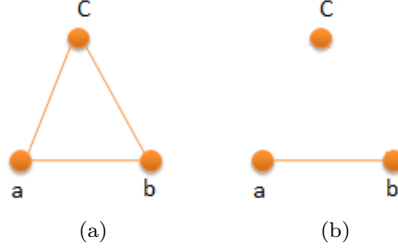


Figure 1: CQSC with one controller, (a) initially shared GHZ-like state among the controller and the communicators Alice and Bob, (b) after the Z basis measurement by the controller C, the particles a and b become entangled.

CQSC 1: Charlie prepares N number of GHZ-like state of the form,

$$|\zeta_{000}\rangle = \frac{1}{2}[|000\rangle + |011\rangle + |110\rangle + |101\rangle]_{abc} \quad (1)$$

This can also be written as,

$$|\zeta_{000}\rangle = \left[\frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}} \right]_{abc} \quad (2)$$

in the Z basis and as

$$|\zeta_{000}\rangle = \frac{1}{2}[|+++\rangle + |--\rangle]_{abc} \quad (3)$$

in the X basis.

Charlie, now, has in his possession a sequence of N number of GHZ-like state $[P_1(a)P_1(b)P_1(c), P_2(a)P_2(b)P_2(c), \dots, P_N(a)P_N(b)P_N(c)]$, where the a,b,c represents three particles in the GHZ-like state and the subscript represents the order.

Charlie divides the sequence into three, ‘a’ sequence : $[P_1(a)P_2(a)P_3(a), \dots, P_N(a)]$, ‘b’ sequence: $[P_1(b)P_2(b)P_3(b), \dots, P_N(b)]$ and ‘c’ sequence: $[P_1(c)P_2(c)P_3(c), \dots, P_N(c)]$. Charlie then sends the ‘a’ sequence to Alice, ‘b’ sequence to Bob and retains the ‘c’ sequence with himself. The communicating parties are already aware of the shared GHZ-like state.

CQSC 2: The controller Charlie randomly selects a sufficiently large subset of particles from his ‘c’ sequence for the first eavesdrop checking. These particles are then measured in either Z or X basis at random. Later the position of the sample particles and the basis chosen for measurement are announced via a public channel. Alice and Bob choose the same basis to measure the corresponding particle in their sequence. When Alice and Bob tell their measurement results to Charlie, he can find out the error rate. From equation 1, if Charlie gets $|0\rangle_c$ in the Z basis measurement, then the results of Alice and Bob are correlated and if Charlie gets $|1\rangle_c$, then their results are anti-correlated. Similarly results corresponding to Charlie’s measurement in X basis are related as given in equation 3. They continue to the next step if the error rate is low, otherwise they abort the communication and start from the first step on a later occasion.

CQSC 3: After the first eavesdrop check, the controller performs Z-basis measurement on the remaining particles in the ‘c’ sequence. This measurement allows the controller to disentangle all particles in the ‘c’ sequence from the sequences ‘a’ and ‘b’. At this stage Alice and Bob share Bell pairs according to equation 2 as is pictorially shown in figure 1. However, Charlie shares his measurement result only with Bob through a classical channel. This allows the receiver to have an advantage over eavesdropper. Now Bob and Charlie alone know which Bell pair is shared between Alice and Bob, since they already have information about the initially shared GHZ-like state.

CQSC 4: To enhance the security, Bob does any one of the four unitary operations $I, \sigma_x, \sigma_z, i\sigma_y$ randomly on his ‘b’ sequence $[P_1(b)P_2(b)P_3(b), \dots, P_N(b)]$ remaining after the first eavesdrop check. These operations transform the Bell states shared between Alice and Bob accordingly. This transformation protects the information about the shared entanglement between the users also from controller’s knowledge. Now, only Bob knows which are the shared Bell pairs. Bob informs Alice that he is ready to receive the message.

Unitary operation performed by Alice	Encoded message
I	00
σ_x	01
σ_z	10
$i\sigma_y$	11

Table 1: Unitary operations and the corresponding encoded message

CQSC 5: After receiving the confirmation from Bob, Alice encodes her secret message to the ‘a’ sequence $[P_1(a)P_2(a)P_3(a), \dots, P_N(a)]$ remaining with her after the first eavesdrop check. For encoding the secret message Alice uses one of the four unitary operations $I, \sigma_x, \sigma_z, i\sigma_y$ and each one corresponding to two bit of information as shown in table 1. Before encoding the message, Alice inserts sufficient decoy photons in her sequence in order to confuse the

eavesdropper in decoding the secret message. This process would improve the security of the protocol. Now Alice sends her encoded ‘a’ sequence along with the decoy photons to Bob through a quantum channel as in the case of dense coding[19].

CQSC 6: After receiving the encoded message sequence from Alice, Bob sends a confirmation signal back to Alice. On receiving the confirmation message from Bob, Alice announces the positions and the basis of the decoy photons. Bob will measure the decoy photons in the respective basis and tells his result to Alice so that she can calculate the error rate. Now, Bob has both the qubits of the EPR pair. On these transformed EPR pairs, Bob performs Bell basis measurements. With the knowledge of the unitary operation that he has earlier done on the ‘b’ sequence before the encoding process and with the Bell measurement results, Bob can obtain the secret message sent by Alice. Since Bob initially changed the state, Eve(the eavesdropper) will get nothing even if she eavesdrops.

For an example, consider that Alice wants to send a 6 bit message, say, 100101 to Bob. Let $|\zeta_{000}\rangle = \frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}}]_{ABC}$ be the GHZ-like state shared among the two users Alice and Bob, and the controller Charlie. They need three sets of GHZ-like state after the first eavesdrop check to send this 6 bit of information. Alice, Bob and Charlie share the set of three GHZ-like state as elaborated in CQSC:1 of our protocol. After the first eavesdrop check as per CQSC:2, Charlie measures his C-sequence as explained in CQSC: 3 and informs Bob about his measurement. Let Charlie’s measurement results be $|0\rangle, |1\rangle$ and $|0\rangle$ so that the shared Bell states between Alice and Bob are $|\phi^+\rangle, |\psi^+\rangle$ and $|\phi^+\rangle$ respectively. Then Bob randomly select any three unitary operations as explained in CQSC:4, which makes him the only user who knows the shared Bell state. For instance, say, Bob selects σ_x, I and σ_z respectively to operate his B sequence, then the shared Bell states transform to $|\psi^+\rangle, |\psi^+\rangle$ and $|\phi^-\rangle$. Now Alice encodes her message on her A sequence using unitary operations as explained in CQSC: 5. To send 100101, she selects σ_z, σ_x and σ_x respectively to operate on her qubits. Alice’s operation transform the Bell pairs to $|\psi^-\rangle, |\phi^+\rangle$ and $|\psi^-\rangle$. Alice sends her encoded sequence to Bob after inserting decoy photons to check error rate as explained in CQSC: 6. After removing the decoy photos Bob does Bell measurement on the Bell pair. His measurement result for this particular example is 110011. With the knowledge of shared Bell pair before encoding the message, Bob can analyse the operation done by Alice and hence gets the secret message 100101.

3 CQSC with two controllers

Here we elaborate our protocol on how to realise the communication between Alice and Bob with the help of two trusted controllers C_1 and C_2 . It requires two sets of GHZ-like states to achieve this two-controller communication. The CQSC scheme is explained in following steps,

2CQSC 1: The controller C_1 prepares N number of two sets of GHZ-like

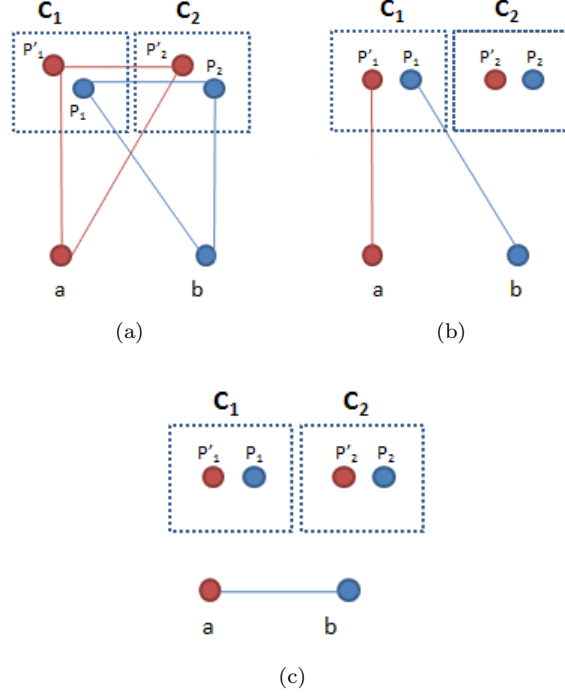


Figure 2: CQSC with two controllers, (a) initially shared GHZ-like states among the two controllers and the communicators, (b) the controller C_2 measures his two particles p_2 and p'_2 in Z basis, this changes the particles p'_1 and a , p_1 and b to Bell pairs, (c) the controller C_1 swaps his particles p_1 and p'_1 , which turns the particles a and b to Bell pair.

state, in the states $|\zeta_1\rangle$ and $|\zeta_2\rangle$.

$$|\zeta_1\rangle = \left[\frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}} \right]_{p'_1 a p'_2} \quad (4)$$

$$|\zeta_2\rangle = \left[\frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}} \right]_{p_1 b p_2} \quad (5)$$

The first set of GHZ-like state is composed of three particles (p'_1 , a and p'_2) and those in second set of GHZ-like state are (p_1 , b and p_2). The ordered sequence of the two set of GHZ-like state is given by $[P_1(p'_1)P_1(a)P_1(p'_2), P_2(p'_1)P_2(a)P_2(p'_2), \dots, P_N(p'_1)P_N(a)P_N(p'_2)]$ and $[P_1(p_1)P_1(b)P_1(p_2), P_2(p_1)P_2(b)P_2(p_2), \dots, P_N(p_1)P_N(b)P_N(p_2)]$. The controller C_1 divides the two set of GHZ-like states into six sequences: $[p'_1, a, p'_2, p_1, b, p_2]$ and distribute the sequences among the users and controllers as follows. Sequences p_2 : $[P_1(p_2)P_2(p_2), \dots, P_N(p_2)]$, p'_2 : $[P_1(p'_2)P_2(p'_2), \dots, P_N(p'_2)]$ are given to the controller C_2 and sequences a : $[P_1(a)P_2(a), \dots, P_N(a)]$, b : $[P_1(b)P_2(b), \dots, P_N(b)]$ are given to the users Alice and Bob respectively. The remaining two sequences c_1 : $[P_1(p_1)P_2(p_1), \dots, P_N(p_1)]$ and p'_1 : $[P_1(p'_1)P_2(p'_1), \dots, P_N(p'_1)]$ are retained by C_1 . The controllers and the two communicating parties are aware of the shared GHZ-like state.

2CQSC 2: The controller C_2 initiates the first eavesdrop check by choosing

a large subset of particles from the sequence p_2 and p'_2 and measures the particles randomly in X or Z basis. Then C_2 announces the measurement basis and the result in a public channel. Based on the information published by C_2 Alice and Bob performs measurement on the corresponding particles in their sequence in same basis as chosen by C_2 . Alice and Bob share their results to the controller C_1 and in turn C_1 measures the corresponding particles in p_1 and p'_1 sequence in the same basis as chosen by C_2 . By comparing the measurement results, C_1 can find the error rate. If the error rate is below the threshold, they continue their communication, otherwise C_1 informs others to abort the communication and start the whole process from the beginning.

2CQSC 3: After the eavesdrop check, the controller C_1 insists C_2 to measure the two particles sequences p_2 and p'_2 in Z basis. As a result of these measurements entanglement is established between pairs (p'_1, a) and (p_1, b) according to equation 4 and 5, as shown in figure: 2(b). After the public announcement of measurement results by controller C_2 , C_1 performs bell measurement on two sequence p_1 and p'_1 in order. This measurement allows entanglement to be established between sequences a and b . The Bell measurement result of C_1 is shared with the receiver Bob and then the communication proceeds as in one controller case as explained in previous section, in step **CQSC 4**. The possible measurement outputs of the two controllers and the shared Bell pair between the sender and receiver is given in table: 2.

C_2 (p'_2 p_2)	C_1 (p'_1 p_1)	Shared bell pair between Alice and Bob
0 0	0 0	$ \phi^+\rangle$
	0 1	$ \psi^+\rangle$
	1 0	$ \phi^-\rangle$
	1 1	$ \psi^-\rangle$
0 1	0 0	$ \psi^+\rangle$
	0 1	$ \phi^+\rangle$
	1 0	$ \psi^-\rangle$
	1 1	$ \phi^-\rangle$
1 0	0 0	$ \psi^+\rangle$
	0 1	$ \phi^+\rangle$
	1 0	$ \psi^-\rangle$
	1 1	$ \phi^-\rangle$
1 1	0 0	$ \phi^+\rangle$
	0 1	$ \psi^+\rangle$
	1 0	$ \phi^-\rangle$
	1 1	$ \psi^-\rangle$

Table 2: CQSC with two controllers

4 CQSC with three controllers

In the case of three controller QSC, we consider C_1 , C_2 and C_3 as the trusted controllers. Here again we need only two sets of GHZ-like state to realise three-party Controlled quantum secure communication between legitimate users. The 3CQSC scheme is explained as follows.

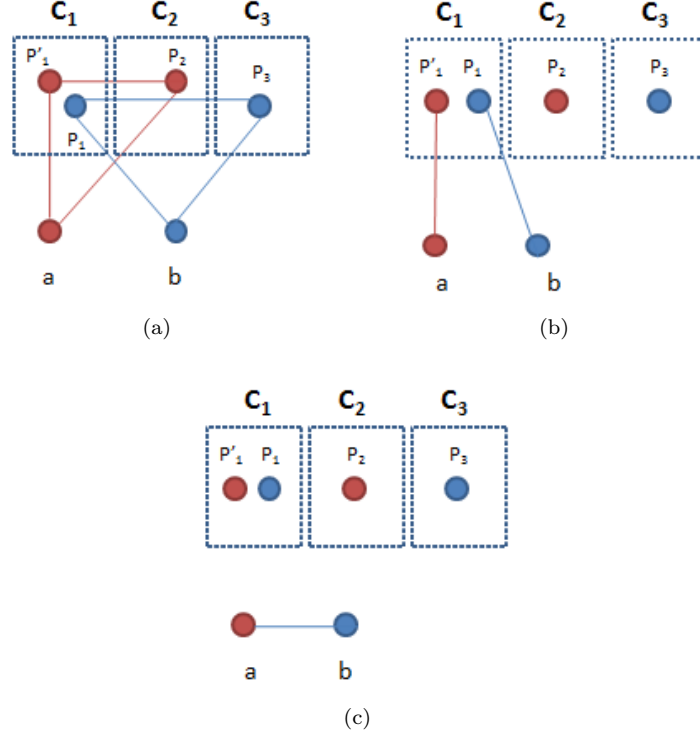


Figure 3: CQSC with three controllers, (a) initially shared GHZ-like states among the three controllers and the communicators, (b) the controller C_2 and C_3 measures their particles p_2 and p_3 in Z basis, this changes the particles p'_1 and a , p_1 and b to Bell pairs, (c) the controller C_1 swaps his particles p_1 and p'_1 , which turns the particles a and b to Bell pair.

3CQSC 1: The controller C_1 prepares N number of two sets of GHZ-like state $\{|\zeta_1\rangle, |\zeta_2\rangle\}$ and distributes the particles among the other controller C_2 , C_3 and the users a and b . Let the two sets of GHZ-like state be,

$$|\zeta_1\rangle = \left[\frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}} \right]_{p'_1 a p_2} \quad (6)$$

$$|\zeta_2\rangle = \left[\frac{(|\phi^+\rangle|0\rangle + |\psi^+\rangle|1\rangle)}{\sqrt{2}} \right]_{p_1 b p_3} \quad (7)$$

where, $(p'_1, a$ and $p_2)$ represents particles that belong to the first set of GHZ-like state $|\zeta_1\rangle$ and particles $(p_1, b$ and $p_3)$ belong to the second set $|\zeta_2\rangle$. Now the controller C_1 divides the N number of GHZ-like states into six sequences: $\{p'_1,$

$a, p_2, p_1, b, p_3\}$ and distributes it among the controllers and users as follows. The sequences $p_2 : [P_1(p_2)P_2(p_2), \dots, P_N(p_2)]$, $p_3 : [P_1(p_3)P_2(p_3), \dots, P_N(p_3)]$ and $a : [P_1(a)P_2(a), \dots, P_N(a)]$, $b : [P_1(b)P_2(b), \dots, P_N(b)]$ are given to Controllers C_2 , C_3 and users a, b respectively. The remaining sequences $c'_1 : [P_1(p'_1)P_2(p'_1), \dots, P_N(p'_1)]$ and $p_1 : [P_1(p_1)P_2(p_1), \dots, P_N(p_1)]$ are retained by the Controller C_1 . Here the shared GHZ-like states are known to the controllers and the two communicating parties.

3CQSC 2: For the first eavesdrop checking, the controllers C_2 and C_3 chooses a large subset of particles with the same order from the sequence p_2, p_3 and measures the particles randomly in X or Z basis. They announce their measurement basis and results in a public channel. Using the obtained information, Alice and Bob chooses the corresponding particles with same order from the sequences a, b and selects measurement basis same as that of C_2 and C_3 respectively. Their measurement results are communicated only with the controller C_1 . Later, C_1 measures the corresponding particles in the p'_1, p_1 sequences with the same order in the basis same as that of C_2 and C_3 respectively. By comparing the results of other users, C_1 can calculate the error rate. If the error rate is low they proceed to the next step, otherwise they abort the communication and start from the beginning.

3CQSC 3: The controllers C_2 and C_3 are instructed to measure their particle sequences p_2 and p_3 in Z basis. The measurement of p_2 allows the Controller C_1 and the sender Alice to share Bell pairs as in equation 6. Similarly the measurement of p_3 allows the Controller C_1 and the receiver Bob to share Bell pairs according to equation 7. The entanglement relation between the particles after the measurements are pictorially shown in figure: 3(b). The controller C_2 and C_3 announce their results publicly. After this announcement the controller C_1 performs bell measurement on the two sequence p_1 and p'_1 with the same order. This in turn swaps the entanglement between C_1 and users to only among user sequences a and b as shown in figure: 3(c). The Bell measurement results of C_1 is shared with the receiver Bob and now the communication proceeds as in one controller case **CQSC 4**. The possible measurement results of the three controllers and the shared Bell pair between the sender and receiver is given in table 3 and is similar as the case of two controllers.

C_3 (p_3)	C_2 (p_2)	C_1 (p'_1 p_1)	Shared bell pair between Alice and Bob
0	0	0 0	$ \phi^+\rangle$
		0 1	$ \psi^+\rangle$
		1 0	$ \phi^-\rangle$
		1 1	$ \psi^-\rangle$
0	1	0 0	$ \psi^+\rangle$
		0 1	$ \phi^+\rangle$
		1 0	$ \psi^-\rangle$
		1 1	$ \phi^-\rangle$
1	0	0 0	$ \psi^+\rangle$
		0 1	$ \phi^+\rangle$
		1 0	$ \psi^-\rangle$
		1 1	$ \phi^-\rangle$
1	1	0 0	$ \phi^+\rangle$
		0 1	$ \psi^+\rangle$
		1 0	$ \phi^-\rangle$
		1 1	$ \psi^-\rangle$

Table 3: CQSC with three controllers

5 Generalized controlled Quantum Secure Communication

In this section, we generalize our protocol for CQSC with N trusted controllers. Let $C_1, C_2, C_3 \dots C_N$ denote the N controllers. The particle distribution of each GHZ-like state among the controllers and total number of GHZ-like states required for establishing the protocol can be found from the equations given below. Here, each line represents an entangled set of GHZ-like state.

For odd number of controllers:

$$\left\{ p'_{\frac{N-1}{2}}, p'_{\frac{N-3}{2}}, p_{\frac{N+1}{2}} \right\} \quad (8)$$

Equation: 8, represents the three particles from the first set of entangled GHZ-like state. The number in subscript represents the identity of each controller and it depends on the total number of odd controllers, N. These particles are sent to different controllers based on the value in the subscript. The remaining set of GHZ-like states is distributed among the controllers according to the following pattern:

$$\left\{ p_{\frac{N-(2m+1)}{2}}, p'_{\frac{N-(2m+5)}{2}}, p_{\frac{N+(2m+3)}{2}} \right\} \quad (9)$$

For different values of m, the above equation generates entangled states which has to be distributed among different controllers. It terminates when the value of the middle term, $(N-(2m+5)/2)$ becomes -1 . Therefore, m varies from $m = \{0, 1, 2, \dots, \frac{N-3}{2}\}$, generating $m + 1$ set of GHZ-like states or $\frac{N-1}{2}$ set. Now, by including the first set given in equation: 8, the total number of

GHZ-like states required for the odd number of controllers case becomes $\frac{N+1}{2}$. On termination, the terms $[p'_0, p'_{-1}]$ are replaced by $[a, b]$ and are send to the legitimate users Alice and Bob respectively.

For even number of controllers:

$$\left\{ p'_{\frac{N}{2}}, p'_{\frac{N-2}{2}}, p'_{\frac{N+2}{2}} \right\} \quad (10)$$

Similar to the odd number case, equation: 10 represents the first set of GHZ-like state. The equation given below generates the remaining set of entangled states depending on the value of m .

$$\left\{ p_{\frac{N-2m}{2}}, p'_{\frac{N-(2m+4)}{2}}, p_{\frac{N+(2m+2)}{2}} \right\} \quad (11)$$

The above sequence of equations also terminate, when the value of middle term $(\frac{N-(2m+4)}{2})$ becomes -1 . This gives the value of m to be varying from $m = \{0, 1, 2, \dots, \frac{N-2}{2}\}$ generating $m+1$ set of GHZ-like state or $\frac{N}{2}$ set. Again by including the entangled state given in equation: 10, the total number of required entangled states can be found to be $\frac{N+2}{2}$. On termination, as in the previous case, the terms $[p'_0, p'_{-1}]$ are replaced by $[a, b]$ and are send to the legitimate users Alice and Bob respectively.

The controller C_1 prepares the required number of GHZ-like states and distribute it among other controllers and users. C_1 retains particle with subscripts corresponding to his identity. After the distribution, C_1 informs the controllers possessing third particle of each GHZ-like state to measure their particle in Z basis, which makes the other two particles of corresponding GHZ-like state collapse to Bell state. C_1 informs the controllers with the first particle of each GHZ-like state to perform Bell measurement with the other particle in their possession. Then the controllers numbering from $C_{\frac{N-1}{2}}$ to C_1 for odd number of controllers and $C_{\frac{N}{2}}$ to C_1 for even number of controllers will perform bell measurement on their respective particles in the decreasing order of controller number given in subscript. After the final Bell measurement from C_1 , an entanglement channel gets established between the users to enable quantum secure communication.

6 Security analysis and efficiency of the proposed CQSC

In this section we are analysing the security of our scheme towards different kinds of eavesdropping attacks. The most common attacks includes; intercept-resend attack, measure-resend attack, entanglement attack etc.

The intercept-resend attack: In this attack, Eve creates N sets of GHZ-like state, say $|\zeta\rangle_{xyz}$. She may capture the a and b sequence that have been sent to Alice and Bob by Charlie in the step **CQSC 1** and replace those a and b sequences with her x and y sequences and resend it to Alice and Bob. However, on the first eavesdropping check, the presence of an eavesdropper can be found from the error rate calculated by Charlie, because of the non-correlation between C sequence of Charlie and x, y sequences of Eve.

Likewise, Eve may again try to intercept the encoded a sequence during its transmission from Alice to Bob. However, in the second eavesdropping check

(CQSC 6) the presence of Eve gets revealed by the disturbance she creates on the decoy photons. The ignorance of Eve, about the position and the basis in which the decoy photons are created, reveals the presence of Eve.

The measure-resend attack: In this case, Eve may measure each particle of a and b sequence during its transmission from Charlie to Alice or Bob. After that she resend those particles to the corresponding users. However, this action performed by Eve will destroy the entangled GHZ-like state and the presence of Eve will get revealed in the first eavesdrop checking. Even if she captures the message encoded a sequence, her lack of knowledge about the position and basis with which the decoy photons are created, reveals her presence in the second eavesdrop check.

The entangle-measure attack: In this type of attack, eavesdropper may try to entangle her ancilla qubits with the travelling qubit sequences a and b sent by Charlie to Alice and Bob respectively. For instance, Eve can entangle her ancilla qubits $|00\rangle_{xy}^{(n)}$ with the particles in the sequences a and b by two CNOT operations. Where, n in the superscript represents the order of ancilla bits. The particles (a, b) act as control bits and (x, y) act as target bits. The appropriate unitary operation U is explicitly given below.

$$\begin{aligned}
U|\Psi\rangle_{abc12} &= CNOT_{(ax)}CNOT_{(by)}\left\{\frac{|\phi^+\rangle_{ab}|0\rangle_c+|\psi^+\rangle_{ab}|1\rangle_c}{\sqrt{2}}\right\}\otimes|00\rangle_{xy} \\
&= \frac{1}{2}\{|00000\rangle+|01101\rangle+|11011\rangle+|10110\rangle\}_{abcxy} \\
&= \frac{1}{\sqrt{2}}\{(|\phi^+\rangle_{ab}|\phi^+\rangle_{xy}+|\phi^-\rangle_{ab}|\phi^-\rangle_{xy})|0\rangle_c \\
&+ (|\psi^+\rangle_{ab}|\psi^+\rangle_{xy}+|\psi^-\rangle_{ab}|\psi^-\rangle_{xy})|1\rangle_c\}
\end{aligned}$$

The entanglement of Eve's particles (x, y) with the qubits (a, b) creates two additional undesired bell state results, which will increase the error in the expected correlations by 50%. Hence in the first eavesdrop checking, Charlie can detect the presence of an eavesdropper 50% of times. Even if Eve tries to entangle her ancilla bits with the message encoded a sequence, Eve will get detected because of the disturbance she creates on decoy photons. Also Eve gets restricted from obtaining any useful information, because of the random unitary operations performed by Bob in his b sequence before Alice encodes her secret message on the a sequence. In our protocol we have supposed that all controllers are trustworthy. The proposed scheme can be made more secure by the inclusion of an identity authentication step between the users, before decoding the message.

Efficiency: Efficiency of the proposed protocol can be calculated using the equation[21],

$$\eta = \frac{c}{q+b} \quad (12)$$

where c is the number of classical bits transmitted, q is the number of qubits used, b is the number of classical bits exchanged. For our scheme $c = 2, q = 3$ and $b = 1$. That is, we will get an efficiency of 50%.

7 Conclusion

We have presented a controlled quantum secure communication protocol using GHZ-like state as quantum channel and employed the dense coding technique to increase the qubit efficiency. The sender Alice and receiver Bob are allowed to communicate only when the controller Charlie allows them. Bob performs random unitary operations on particle in his possession to secure the information about shared entanglement, from the controller's knowledge. Alice encodes her secret messages on particles in her possession by performing one of four different unitary operations, each corresponding to a different two bit message, and transmits it to Bob. By performing Bell measurement on particles in his possession, Bob read out the secret messages.

Further, we have generalized our scheme to N-controllers using a set of similar GHZ-like states. In this multiparty controlled quantum secure communication, one of the controller prepares and efficiently distributes the entangled states among the other controllers. The users then require the co-operation from N controllers to begin their secret communication, which may be useful in many practical applications. We have also shown that our protocol is secure against common eavesdropping attacks and the qubit efficiency found to be 50%, which is relatively higher than other existing QSDC schemes. Our protocol is feasible with the current technology as it requires only single particle measurements and entanglement swapping to establish secure communication channel between users. However, our protocol demands all the controllers to be trustworthy for successful communication.

Acknowledgements

One of the author Jemy thank Sarath R for his valuable comments on the manuscript.

References

- [1] Bennett C.H., Brassard G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the International Conference on Computers, Systems and Signal Processing Bangalore press, India, pp. 175–179 (1984).
- [2] Boström K., Felbinger T., Phys. Rev. Lett., 89, 187902 (2002).
- [3] Wang C., Deng F.G., Long G.L., Opt. Commun. 253, 15-20 (2005).
- [4] Wang C., Deng F.G., Li Y.S., Liu X.S., Long G.L., Phys. Rev. A, 71, 044305 (2005).
- [5] Gao T., Yan F.L., Wang Z.X., J. Phys. A Math. Gen. 38, 5761-5770 (2005).
- [6] Yan F.L., Zhang X.Q., Eur. Phys. J. B, 41, 75-78 (2004).
- [7] Zhong-Xiao M., Zhan-Jun Z., Yong L., Chin. Phys. Lett., 22, 18 (2005).
- [8] Banerjee A., Pathak A., Phys. Lett. A, 376, 2944-2950 (2012).

- [9] Hassanpour S., Houshmand M., Quantum Inf Process., 14, 739-753 (2015).
- [10] Pathak A., Quantum Inf Process., 14, 2195-2210 (2015).
- [11] Deng F.G., Long G.L., Liu X.S., Phys. Rev. A, 68, 042317 (2003).
- [12] Xiao-Long Z., Yue-Xia Z., Hua W., Chin. Phys. B, 18, 435 (2009).
- [13] Dong L., Xiu X.M., Gao Y.J., Ren Y.P., Liu H.W., Opt. Commun., 284, 905-908 (2011).
- [14] Hai-Jing C., He-Shan S., Chin. Phys. Lett., 23, 290 (2006).
- [15] Jian W., Quan Z., Chao-Jing T., Commun. Theor. Phys., 48, 637 (2007).
- [16] Gao F., Qin S.J., Wen Q.Y., Zhu F.C., Opt. Commun., 283, 192-195 (2010).
- [17] Yang K., Huang L., Yang W., Song F., Int. J. Theor. Phys., 48, 516-521 (2009).
- [18] Banerjee A., Patel K., Pathak A., Int. J. Theor. Phys., 50, 507-510 (2011).
- [19] Bennett C.H., Wiesner S.J., Phys. Rev. Lett., 69, 2881 (1992).
- [20] Hsieh C.R., Tasi C.W., Hwang T., Commun. Theor. Phys., 54, 1019 (2010).
- [21] Wen-Jie L., Han-Wu C., Ting-Huai M., Zhi-Qiang L., Zhi-Hao L., Wen-Bo H., Chin. Phys. B, 18, 4105 (2009).